PROCESSOR

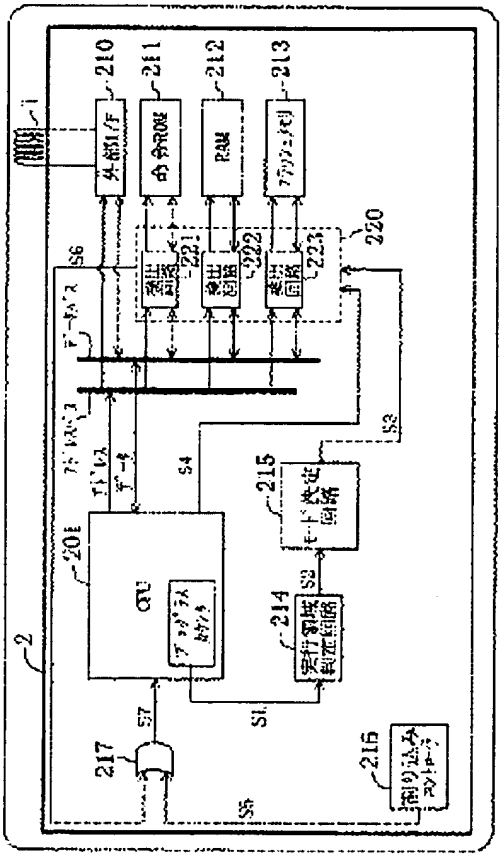
Publication number: JP2004145605
Publication date: 2004-05-20
Inventor: HASEBE TOMOYA
Applicant: MATSUSHITA ELECTRIC IND CO LTD
Classification:
- international: ***G06F1/00; G06F12/14; G06K19/073;*** **G06F1/00; G06F12/14; G06K19/073;** (IPC1-7): G06F12/14; G06F1/00; G06K19/073
- european:
Application number: JP20020309276 20021024
Priority number(s): JP20020309276 20021024

Abstract of **JP2004145605**

PROBLEM TO BE SOLVED: To provide a mechanism that prevents unauthorized reading from an instruction ROM and unauthorized reading/writing from/into a data memory all by an added program when a program is externally added to an extended memory, in a processor having an instruction ROM, a data memory, an extended memory and an external I/F.

SOLUTION: An operation mode is set for every region where a program counter of an instruction processed by a CPU belongs, and access to each region is restricted in dependence on every operation mode. If unauthorized access detection circuits 221 to 223 for detecting unauthorized access detect unauthorized access, an interrupt is generated to stop the processing and prevent unauthorized access by an added program.

COPYRIGHT: (C)2004,JPO



(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-145605
(P2004-145605A)
(43)公開日　平成16年5月20日(2004.5.20)

(51)Int.Cl.[7]	F I		テーマコード（参考）
G06F 12/14	G06F 12/14	310H	5B017
G06F 1/00	G06F 9/06	660L	5B035
G06K 19/073	G06K 19/00	P	5B076

審査請求 未請求　請求項の数 9　OL　（全 17 頁）

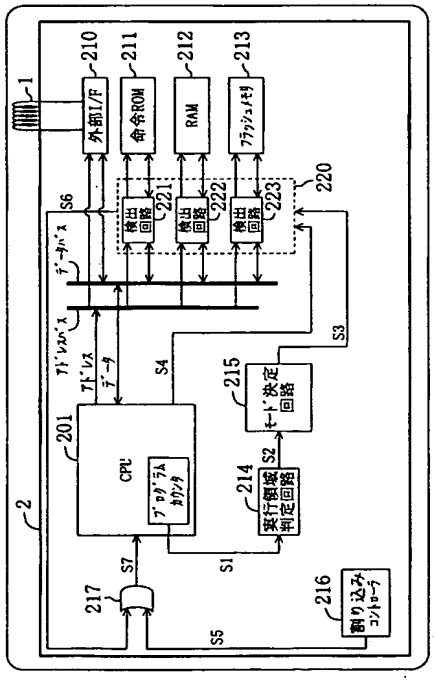
(21)出願番号　特願2002-309276(P2002-309276)
(22)出願日　平成14年10月24日(2002.10.24)

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真１００６番地
(74)代理人　100077931
弁理士　前田　弘
(74)代理人　100094134
弁理士　小山　廣毅
(74)代理人　100110939
弁理士　竹内　宏
(74)代理人　100110940
弁理士　嶋田　高久
(74)代理人　100113262
弁理士　竹内　祐二
(74)代理人　100115059
弁理士　今江　克実

最終頁に続く

(54)【発明の名称】プロセッサ

(57)【要約】
【課題】命令ＲＯＭとデータメモリと拡張メモリと外部Ｉ／Ｆをもつプロセッサにおいて、外部から拡張メモリにプログラムが追加された場合において、追加されたプログラムによる命令ＲＯＭに対する不正読み出しやデータメモリに対する不正読み書きを防止する機構を提供する。
【解決手段】ＣＰＵが処理を行う命令のプログラムカウンタの属する領域ごとに動作モードを設け、その動作モードごとに各領域へのアクセス制限を設ける。不正アクセスを検出する不正アクセス検出回路２２１～２２３によって、不正なアクセスを検出した場合には割り込みを発生させて、処理を中止させることによって、追加されたプログラムによる不正アクセスを防ぐ。
【選択図】　図１



【特許請求の範囲】
【請求項1】
外部とのデータのやりとりを行う外部Ｉ／Ｆと、
プログラムを格納する命令ＲＯＭと、
データを格納するデータメモリと、
前記外部Ｉ／Ｆを経由して追加されたプログラムを格納する拡張メモリと、
前記命令ＲＯＭおよび前記拡張メモリに格納されたプログラムを実行するＣＰＵと、
前記ＣＰＵが実行している命令のプログラムカウンタ値に基づいて実行領域を判定する実行領域判定回路と、
前記実行領域判定回路による判定結果に従って動作モードを決定するモード決定回路と、
前記モード決定回路によって決定された動作モードとアクセスアドレスとによって許可されないアクセスが発生した場合に割り込み要求を出力する不正アクセス検出回路とを備える
ことを特徴とするプロセッサ。
【請求項２】
請求項１において、
前記モード決定回路によって決定される動作モードには、特権モード、ＡＰＩモード、ユーザモードが含まれ、
論理アドレス空間は、特権領域、ＡＰＩ領域、ユーザ領域の３つに区分され、
前記命令ＲＯＭには前記特権領域および前記ＡＰＩ領域、前記データメモリには前記特権領域、前記ＡＰＩ領域および前記ユーザ領域、前記拡張メモリには前記ユーザ領域が割り当てられ、
前記モード決定回路は動作モードを、前記特権領域上のプログラム実行時には特権モード、前記ＡＰＩ領域上のプログラム実行時にはＡＰＩモード、前記ユーザー領域上のプログラム実行時にはユーザモードとする
ことを特徴とするプロセッサ。
【請求項３】
請求項２において、
前記不正アクセス検出回路は、
前記モード決定回路によって決定された動作モードが特権モードのとき、前記特権領域、前記ＡＰＩ領域および前記ユーザ領域へのデータアクセスおよび命令アクセスを許可し、
前記モード決定回路によって決定された動作モードがＡＰＩモードのとき、前記特権領域への命令アクセスと、前記ＡＰＩ領域および前記ユーザ領域へのデータアクセスおよび命令アクセスとを許可し、前記特権領域へのデータアクセスを禁止し、
前記モード決定回路によって決定された動作モードがユーザモードのとき、前記ＡＰＩ領域への命令アクセスと、前記ユーザ領域へのデータアクセスおよび命令アクセスとを許可し、前記特権領域へのデータアクセスおよび命令アクセスと、前記ＡＰＩ領域へのデータアクセスとを禁止する
ことを特徴とするプロセッサ。
【請求項４】
外部とのデータのやりとりを行う外部Ｉ／Ｆと、
プログラムを格納する命令ＲＯＭと、
データを格納するデータメモリと、
前記外部Ｉ／Ｆを経由して追加されたプログラムを格納する拡張メモリと、
前記命令ＲＯＭおよび前記拡張メモリに格納されたプログラムを実行するＣＰＵと、
前記ＣＰＵが実行している命令のプログラムカウンタ値に基づいて実行領域を判定する実行領域判定回路と、
特権フラグと、
前記特権フラグの値を判定する特権フラグ判定回路と、
前記実行領域判定回路による判定結果と前記特権フラグ判定回路による判定結果とに従っ

て動作モードを決定するモード決定回路と、
前記モード決定回路によって決定された動作モードとアクセスアドレスとによって許可されないアクセスが発生した場合に割り込み要求を出力する不正アクセス検出回路とを備える
ことを特徴とするプロセッサ。
【請求項５】
請求項４において、
前記モード決定回路によって決定される動作モードには、特権モード、ＡＰＩモード、ユーザモードが含まれ、
論理アドレス空間は、特権領域、ＡＰＩ領域、ユーザ領域に区分され、
前記命令ＲＯＭには前記特権領域および前記ＡＰＩ領域、前記データメモリには前記特権領域、前記ＡＰＩ領域および前記ユーザ領域、前記拡張メモリには前記ユーザ領域、前記特権フラグには前記ＡＰＩ領域が割り当てられ、
前記モード決定回路は動作モードを、前記特権領域または前記ＡＰＩ領域上のプログラム実行時でありかつ前記特権フラグがＯＮのときには特権モード、前記ＡＰＩ領域上のプログラム実行時でありかつ前記特権フラグＯＦＦのときにはＡＰＩモード、前記ユーザー領域上のプログラム実行時にはユーザモードとする
ことを特徴とするプロセッサ。
【請求項６】
請求項５において、
前記不正アクセス検出回路は、
前記モード決定回路によって決定された動作モードが特権モードのとき、前記特権領域、前記ＡＰＩ領域および前記ユーザ領域へのデータアクセスおよび命令アクセスを許可し、
前記モード決定回路によって決定された動作モードがＡＰＩモードのとき、前記ＡＰＩ領域へのデータアクセスおよび命令アクセスと、前記ユーザ領域へのデータアクセスおよび命令アクセスとを許可し、前記特権領域へのデータアクセスおよび命令アクセスを禁止し、
前記モード決定回路によって決定された動作モードがユーザモードのとき、前記ＡＰＩ領域への命令アクセスと、前記ユーザ領域へのデータアクセスおよび命令アクセスとを許可し、前記特権領域へのデータアクセスおよび命令アクセスと、前記ＡＰＩ領域へのデータアクセスとを禁止する
ことを特徴とするプロセッサ。
【請求項７】
外部とのデータのやりとりを行う外部Ｉ／Ｆと、
プログラムを格納する命令ＲＯＭと、
データを格納するデータメモリと、
前記外部Ｉ／Ｆを経由して追加されたプログラムを格納する拡張メモリと、
前記命令ＲＯＭおよび前記拡張メモリに格納されたプログラムを実行するＣＰＵと、
前記ＣＰＵが実行している命令のプログラムカウンタ値に基づいて実行領域を判定する実行領域判定回路と、
特権フラグと、
Ｎ個（Ｎは２以上の整数）のユーザフラグと、
前記特権フラグの値を判定する特権フラグ判定回路と、
前記ユーザフラグの値を判定するユーザフラグ判定回路と、
前記実行領域判定回路による判定結果と前記特権フラグ判定回路による判定結果と前記ユーザフラグ判定回路による判定結果とに従って動作モードを決定するモード決定回路と、
前記モード決定回路によって決定された動作モードとアクセスアドレスとによって許可されないアクセスが発生した場合に割り込み要求を出力する不正アクセス検出回路とを備える
ことを特徴とするプロセッサ。

【請求項８】
請求項７において、
前記モード決定回路によって決定される動作モードには、特権モード、ＡＰＩモード、ユーザモードが含まれ、
論理アドレス空間は、特権領域、ＡＰＩ領域、第１から第Ｎのユーザ領域に区分され、
前記命令ＲＯＭには前記特権領域および前記ＡＰＩ領域、前記データメモリには前記特権領域、前記ＡＰＩ領域および前記第１から第Ｎのユーザ領域、前記拡張メモリには前記第１から第Ｎのユーザ領域、前記特権フラグにはＡＰＩ領域、前記第１から第Ｎのユーザフラグには前記第１から第Ｎのユーザ領域が割り当てられ、
前記モード決定回路は動作モードを、前記特権領域または前記ＡＰＩ領域上のプログラム実行時でありかつ前記特権フラグがＯＮのときには特権モード、前記ＡＰＩ領域上のプログラム実行時でありかつ前記特権フラグがＯＦＦのときはＡＰＩモード、第Ｍ（１≦Ｍ≦Ｎ）のユーザ領域上のプログラム実行時でありかつ第ＭのユーザフラグがＯＮのとき第Ｍのユーザモードとする
ことを特徴とするプロセッサ。
【請求項９】
請求項８において、
不正アクセス検出回路は、
前記モード決定回路によって決定された動作モードが特権モードのとき、前記特権領域、前記ＡＰＩ領域および前記第１から第Ｎのユーザ領域へのデータアクセスおよび命令アクセスを許可し、
前記モード決定回路によって決定された動作モードがＡＰＩモードのとき、前記ＡＰＩ領域へのデータアクセスおよび命令アクセスと、前記第１から第Ｎのユーザ領域へのデータアクセスおよび命令アクセスとを許可し、前記特権領域へのデータアクセスおよび命令アクセスを禁止し、
前記モード決定回路によって決定された動作モードが前記第Ｍのユーザモードのとき、前記ＡＰＩ領域への命令アクセスと、前記第Ｍのユーザ領域へのデータアクセスおよび命令アクセスとを許可し、前記特権領域へのデータアクセスおよび命令アクセスと、前記ＡＰＩ領域へのデータアクセスと、前記第１から第Ｎのユーザ領域のうち前記Ｍのユーザ領域以外の領域へのデータアクセスおよび命令アクセスとを禁止する
ことを特徴とするプロセッサ。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
この発明はプロセッサに関し、さらに詳しくは、メモリ保護機能を有するプロセッサに関する。
【０００２】
【従来の技術および発明が解決しようとする課題】
近年、流通・サービス分野や交通分野などでＩＣカードが普及しつつある。ＩＣカードには、ユーザプログラム（アプリケーションプログラム）をダウンロードして実行可能なものがある。このようなＩＣカードには書き換え可能な不揮発性メモリ（たとえばフラッシュメモリ）が内蔵されており、この不揮発性メモリにユーザプログラムがダウンロードされる。上述のＩＣカードにはさらに命令ＲＯＭ（読み出し専用不揮発性メモリ）・データＲＡＭ・ＣＰＵが内蔵されている。命令ＲＯＭにはＯＳやサービスプログラムが格納される。命令ＲＯＭおよび書き換え可能な不揮発性メモリに格納されたプログラムに従ってＣＰＵが各種の処理を行う。
【０００３】
しかしながら上述のＩＣカードでは、書き換え可能な不揮発性メモリにダウンロードしたユーザプログラムによって命令ＲＯＭ上のプログラムを不正に読み出したりデータＲＡＭ上のデータを不正に読み出し／書き込んだりすることが可能でありセキュリティが十分に

は確保されない。
【０００４】
この発明の目的は、セキュリティを高めることができるプロセッサを提供することである。
【０００５】
【特許文献１】
特開２０００－７６１３５号公報
【特許文献２】
特開２００２－９１８２６号公報
【特許文献３】
特開平１１－２３８０１６号公報
【０００６】
【課題を解決するための手段および発明の効果】
この発明によるプロセッサは、データ・演算処理を行うＣＰＵと、プログラムを格納する命令ＲＯＭと、データを格納するデータＲＡＭと、外部とのデータのやりとりを行う外部Ｉ／Ｆと、外部Ｉ／Ｆを経由してプログラムを格納する拡張メモリと、ＣＰＵから出力される実行している命令のプログラムカウンタ値にしたがって動作モードを決定するモード決定回路と、モード決定回路からの出力と命令ＲＯＭ、データＲＡＭ、拡張メモリへのアクセスアドレス情報にしたがって不正なアクセスを検出する不正アクセス検出回路から構成され、メモリ領域を特権領域、ＡＰＩ領域、ユーザ領域の３つに区分し、実行プログラムが配置されている領域にしたがってアクセス可能領域を設け、不正なアクセスが検出された場合は割り込みを発生させることを特徴とする。これにより、外部から追加されたプログラムからのセキュリティを確保することができる。
【０００７】
【発明の実施の形態】
以下、この発明の実施の形態を図面を参照して詳しく説明する。なお、図中同一または相当部分には同一の符号を付しその説明は繰り返さない。
【０００８】
（第１の実施形態）
＜ＩＣカードの全体構成＞
第１の実施形態によるＩＣカードの構成を図１に示す。このＩＣカードは非接触型のＩＣカードであり、アンテナコイル１とプロセッサ（ＩＣチップ）２とを備える。プロセッサ２は、ＣＰＵ２０１と、外部インタフェース（Ｉ／Ｆ）２１０と、命令ＲＯＭ（読み出し専用不揮発性メモリ）２１１と、ＲＡＭ２１２と、フラッシュメモリ（書き換え可能な不揮発性メモリ）２１３と、不正アクセス検出回路群２２０と、実行領域判定回路２１４と、モード決定回路２１５と、割り込みコントローラ２１６と、ＯＲ回路２１７とを備える。
【０００９】
アンテナコイル１は、電磁結合によってリーダライタ（図示せず）から電力を受信しかつ情報の送受信を行う。外部Ｉ／Ｆ２１０は、プロセッサ２と外部（アンテナコイル１）との間のインタフェースである。
【００１０】
命令ＲＯＭ２１１には特権プログラム（ＯＳやサービスプログラムなど）が格納される。フラッシュメモリ２１３にはユーザプログラム（アプリケーションプログラム）が格納される。フラッシュメモリ２１３に格納されるユーザプログラムはリーダライタ（図示せず）からアンテナコイル１および外部Ｉ／Ｆ２１０を介してダウンロードされる。
【００１１】
ＣＰＵ２０１は、命令ＲＯＭ２１１およびフラッシュメモリ２１３に格納されているプログラムを実行する。ＣＰＵ２０１は、実行している命令のプログラムカウンタ（ＰＣ）値Ｓ１を出力する。ＣＰＵ２０１は、実行すべきメモリアクセスが命令アクセスであるかデ

ータアクセスであるかを示す信号Ｓ４を出力する。ここでいう「命令アクセス」とは、実行すべき命令を読み込む（命令フェッチ）ためのメモリアクセスのことである。また「データアクセス」とは、読み込んだ命令の内容にメモリへのアクセスが含まれている場合におけるその命令の実行としてのメモリアクセスのことである。ＣＰＵ２０１の内部には命令フェッチを制御する部分とデータアクセスを制御する部分とが存在する。命令フェッチを制御する部分からは命令フェッチ要求が発生し、データアクセスを制御する部分からはデータアクセス要求が発生する。ＣＰＵ２０１は、これらの要求に応答してメモリアクセスを行う。命令フェッチ要求に応答してメモリアクセスを行うときＣＰＵ２０１は、命令アクセスを示す信号Ｓ４を出力する。データアクセス要求に応答してメモリアクセスを行うときＣＰＵ２０１は、データアクセスを示す信号Ｓ４を出力する。

【００１２】

実行領域判定回路２１４は、ＣＰＵ２０１によって実行されている命令が格納されている領域をプログラムカウンタ値Ｓ１に基づいて判定する。領域の種類および区分については後に説明する。実行領域判定回路２１４は、判定された領域を示す信号Ｓ２を出力する。

【００１３】

モード決定回路２１５は、実行領域判定回路２１４からの信号Ｓ２に基づいて動作モードを決定する。動作モードの種類については後に説明する。モード決定回路２１５は、決定した動作モードを示す信号Ｓ３を出力する。

【００１４】

不正アクセス検出回路群２２０は検出回路２２１～２２３を含む。検出回路２２１は、ＣＰＵ２０１から命令ＲＯＭ２１１へのアクセスアドレスと信号Ｓ３～Ｓ４とに基づいて、ＣＰＵ２０１から命令ＲＯＭ２１１へのアクセスを許可／禁止する。検出回路２２２は、ＣＰＵ２０１からＲＡＭ２１２へのアクセスアドレスと信号Ｓ３～Ｓ４とに基づいて、ＣＰＵ２０１からＲＡＭ２１２へのアクセスを許可／禁止する。検出回路２２３は、ＣＰＵ２０１からフラッシュメモリ２１３へのアクセスアドレスと信号Ｓ３～Ｓ４とに基づいて、ＣＰＵ２０１からフラッシュメモリ２１３へのアクセスを許可／禁止する。アクセスを許可するとき検出回路２２１～２２３は、ＣＰＵ２０１からのアクセスアドレスを命令ＲＯＭ２１１・ＲＡＭ２１２・フラッシュメモリ２１３へ与え、当該アドレスへのアクセス（書き込み／読み出し）を行う。アクセスを禁止するとき検出回路２２１～２２３は、ＣＰＵ２０１からのアクセスアドレスを命令ＲＯＭ２１１・ＲＡＭ２１２・フラッシュメモリ２１３へ与えず、検出信号Ｓ６を出力する。

【００１５】

ＯＲ回路２１７は、割り込みコントローラ２１６からの割り込み信号Ｓ５と検出回路２２１～２２３からの検出信号Ｓ６との論理和を割り込み信号Ｓ７としてＣＰＵ２０１に与える。ＣＰＵ２０１は、ＯＲ回路２１７からの割り込み信号Ｓ７に応答して割り込み処理を行う。

【００１６】

＜論理アドレス空間＞

図１に示したＩＣカードの論理アドレス空間を図２に示す。論理アドレス空間は、特権領域と、ＡＰＩ領域と、ユーザ領域とに区分されている。アドレスａ３～ａ４，ａ７～ａ８が特権領域に割り当てられる。アドレスａ５～ａ６，ａ９～ａ１０がＡＰＩ領域に割り当てられる。アドレスａ１～ａ２，ａ１１～ａ１２，ａ１３～ａ１４がユーザ領域に割り当てられる。外部Ｉ／Ｆ２１０にはアドレスａ１～ａ２（ユーザ領域）が割り当てられる。命令ＲＯＭ２１１にはアドレスａ３～ａ４（特権領域），ａ５～ａ６（ＡＰＩ領域）が割り当てられる。ＲＡＭ２１２にはアドレスａ７～ａ８（特権領域），ａ９～ａ１０（ＡＰＩ領域），ａ１１～ａ１２（ユーザ領域）が割り当てられる。フラッシュメモリ２１３にはアドレスａ１３～ａ１４（ユーザ領域）が割り当てられる。

【００１７】

＜メモリ保護機能＞

次に、図１に示したＩＣカードの動作について説明する。

【００１８】
ＩＣカードのＲＯＭ２１１には、ＯＳやサービスプログラムなどの特権プログラムがあらかじめ格納されている。この特権プログラムはＩＣカードの発行者によって保証されているプログラムである。ＩＣカードのユーザは、所望のユーザプログラムをフラッシュメモリ２１３にダウンロードする。フラッシュメモリ２１３にダウンロードされたユーザプログラムは、ＲＯＭ２１１に格納されているＯＳ上で動作する。
【００１９】
ＣＰＵ２０１は、命令ＲＯＭ２１１およびフラッシュメモリ２１３に格納されているプログラムを実行する。ＣＰＵ２０１はパイプライン処理を行う。パイプラインの段数は５段である。命令フェッチステージでは命令のフェッチ、デコードステージでは命令のデコード、実行ステージでは命令の実行、データアクセスステージではデータアクセス、ライトバックステージでは実行結果のレジスタへの書き込みがそれぞれ行われる。
【００２０】
実行領域判定回路２１４は、デコードステージで処理されている命令が格納されている領域（実行領域）を示す信号Ｓ２を出力する。デコードステージで処理されている命令に対応するプログラムカウンタ値Ｓ１がアドレスａ３～ａ４に属するとき実行領域判定回路２１４は、特権領域を示す信号Ｓ２を出力する（図２参照）。デコードステージで処理されている命令に対応するプログラムカウンタ値Ｓ１がアドレスａ５～ａ６に属するとき実行領域判定回路２１４は、ＡＰＩ領域を示す信号Ｓ２を出力する（図２参照）。デコードステージで処理されている命令に対応するプログラムカウンタ値Ｓ１がアドレスａ１３～ａ１４に属するとき実行領域判定回路２１４は、ユーザ領域を示す信号Ｓ２を出力する（図２参照）。
【００２１】
モード決定回路２１５は、動作モードを示す信号Ｓ３を出力する。図３に示すように、実行領域判定回路２１４からの信号Ｓ２が特権領域を示すときモード決定回路２１５は、特権モードを示す信号Ｓ３を出力する。信号Ｓ２がＡＰＩ領域を示すときモード決定回路２１５は、ＡＰＩモードを示す信号Ｓ３を出力する。信号Ｓ２がユーザ領域を示すときモード決定回路２１５は、ユーザモードを示す信号Ｓ３を出力する。このように、デコードステージで処理されている命令が格納されている領域（実行領域）に基づいて動作モードが決定される。
【００２２】
検出回路２２１～２２３は、モード決定回路２１５からの信号Ｓ３が示す動作モードと、ＣＰＵ２０１からのアクセスアドレスが属する領域（アクセス領域）と、信号Ｓ４が示すアクセス種別（データアクセス，命令アクセス）とに基づいてメモリ２１１～２１３へのアクセスを許可／禁止する。具体的には図４に示すように、動作モードが特権モードのとき検出回路２２１～２２３はアクセス領域（特権領域，ＡＰＩ領域，ユーザ領域）およびアクセス種別にかかわらずメモリ２１１～２１３へのアクセスを許可する。動作モードがＡＰＩモードのとき検出回路２２１～２２３は、メモリ２１１～２１３の特権領域へのデータアクセスを禁止し、それ以外のメモリアクセス（特権領域への命令アクセス、ＡＰＩ領域へのデータアクセスおよび命令アクセス、ユーザ領域へのデータアクセスおよび命令アクセス）を許可する。動作モードがユーザモードのとき検出回路２２１～２２３は、特権領域へのデータアクセスおよび命令アクセスとＡＰＩ領域へのデータアクセスとを禁止し、ＡＰＩ領域への命令アクセスとユーザ領域へのデータアクセスおよび命令アクセスとを許可する。
【００２３】
図５はメモリアクセス時のフローチャートである。
【００２４】
ユーザモードのとき、メモリアクセスが特権領域へのアクセスの場合（ＳＴ１１でＹＥＳ）、不正アクセスとして割り込みが発生する（ＳＴ１２）。したがって、ユーザ領域から特権領域へ直接に分岐することはできない。ＡＰＩ領域へのアクセスの場合（ＳＴ１３で

ＹＥＳ）、それがデータアクセスであれば不正アクセスとして割り込みが発生し（ＳＴ１４～ＳＴ１５）、命令アクセスであればＡＰＩ領域への命令アクセスを実行する（ＳＴ１４，ＳＴ１７）。ユーザ領域へのアクセスであれば（ＳＴ１６）、アクセスを実行する（ＳＴ１７）。

【００２５】

ＡＰＩモードのとき、メモリアクセスが特権領域へのアクセスの場合（ＳＴ２１でＹＥＳ）、それがデータアクセスであれば（ＳＴ２２でＹＥＳ）、不正アクセスとして割り込みが発生し（ＳＴ２３）、命令アクセスであれば（ＳＴ２２でＮＯ）特権領域への命令アクセスを実行する（ＳＴ２５）。ＡＰＩ領域またはユーザ領域へのアクセスであれば（ＳＴ２４）、アクセスを実行する（ＳＴ２５）。

【００２６】

特権モードのとき、どの領域に対しても制限なくアクセスを実行する（ＳＴ３１）。

【００２７】

図６は動作モード遷移時のパイプラインチャート図である。図６に示すように、ユーザ領域からＡＰＩ領域への分岐、ＡＰＩ領域から特権領域への分岐の際に、それぞれユーザモードでのＡＰＩ領域へのメモリアクセス、ＡＰＩモードでの特権領域へのメモリアクセスが発生するが、ともに命令アクセスであるのでアクセスは許可される。

【００２８】

＜効果＞

以上のように第１の実施形態では、実行しているプログラムが格納されている領域とアクセス種別（命令アクセス／データアクセス）とに応じてメモリ２１１～２１３へのアクセスを制限している。具体的には、メモリ２１１～２１３の論理アドレス空間を特権領域とユーザ領域とＡＰＩ領域とに分割し、ユーザ領域から特権領域への分岐の際には必ずＡＰＩ領域を経由するようにしている。特権領域およびＡＰＩ領域のプログラムは命令ＲＯＭ２１１に存在し、このプログラムはＩＣカード発行者によって保証された（正しい）プログラムである。ＡＰＩ領域を経由して特権領域に分岐することによって、特権領域中の決められた番地にのみ分岐することを保証している。これにより、ユーザ領域上のプログラムによる特権領域への不正アクセスを防ぐことができる。すなわち特権領域のプログラムおよびデータをユーザプログラムから保護することができる。

【００２９】

（第２の実施形態）

＜ＩＣカードの全体構成＞

第２の実施形態によるＩＣカードの構成を図７に示す。このＩＣカードは、図１に示したＩＣカードの構成に加えてさらに検出回路２２４と、特権フラグ２３１と、特権フラグ判定回路２３２とを備える。

【００３０】

特権フラグ判定回路２３２は、特権フラグ２３１の出力に従って特権フラグのＯＮ／ＯＦＦを判定し、判定結果（特権フラグ２３１がＯＮであるかＯＦＦであるか）を示す信号Ｓ８を出力する。

【００３１】

モード決定回路２１５は、実行領域判定回路２１４からの信号Ｓ２と特権フラグ判定回路２３２からの信号Ｓ８とに基づいて動作モードを決定する。

【００３２】

検出回路２２４は、ＣＰＵ２０１から特権フラグ２３１へのアクセスアドレスと信号Ｓ３～Ｓ４とに基づいて、ＣＰＵ２０１から特権フラグ２３１へのアクセスを許可／禁止する。アクセスを禁止するとき検出回路２２４は検出信号Ｓ６を出力する。

【００３３】

＜論理アドレス空間＞

図７に示したＩＣカードの論理アドレス空間を図８に示す。外部Ｉ／Ｆ２１０、命令ＲＯＭ２１１、ＲＡＭ２１２およびフラッシュメモリ２１３については第１の実施形態と同様

である（図２参照）。ここではさらにアドレスａ１５がＡＰＩ領域に割り当てられる。特権フラグ２３１にアドレスａ１５（ＡＰＩ領域）が割り当てられる。

【００３４】

＜メモリ保護機能＞

次に、図７に示したＩＣカードの動作について説明する。ここでは第１の実施形態と異なる部分について説明する。

【００３５】

モード決定回路２１５は、動作モードを示す信号Ｓ３を出力する。図９に示すように、実行領域判定回路２１４からの信号Ｓ２が特権領域を示しかつ特権フラグ判定回路２３２からの信号Ｓ８が特権フラグ２３１がＯＮであることを示すときモード決定回路２１５は、特権モードを示す信号Ｓ３を出力する。信号Ｓ２がＡＰＩ領域を示しかつ信号Ｓ８が特権フラグ２３１がＯＮであることを示すときモード決定回路２１５は、特権モードを示す信号Ｓ３を出力する。信号Ｓ２がＡＰＩ領域を示しかつ信号Ｓ８が特権フラグ２３１がＯＦＦであることを示すときモード決定回路２１５は、ＡＰＩモードを示す信号Ｓ３を出力する。信号Ｓ２がユーザ領域を示しかつ信号Ｓ８が特権フラグがＯＦＦであることを示すときモード決定回路２１５は、ユーザモードを示す信号Ｓ３を出力する。このように、デコードステージで処理されている命令が格納されている領域（実行領域）と特権フラグ２３１のＯＮ／ＯＦＦとに基づいて動作モードが決定される。

【００３６】

検出回路２２１～２２４は、モード決定回路２１５からの信号Ｓ３が示す動作モードと、ＣＰＵ２０１からのアクセスアドレスが属する領域（アクセス領域）と、信号Ｓ４が示すアクセス種別（データアクセス，命令アクセス）とに基づいてメモリ２１１～２１３および特権フラグ２３１へのアクセスを許可／禁止する。具体的には図１０に示すように、動作モードが特権モードのとき検出回路２２１～２２４はアクセス領域（特権領域，ＡＰＩ領域，ユーザ領域）およびアクセス種別にかかわらずメモリ２１１～２１３および特権フラグ２３１へのアクセスを許可する。動作モードがＡＰＩモードのとき検出回路２２１～２２４は、特権領域へのデータアクセスおよび命令アクセスを禁止し、ＡＰＩ領域へのデータアクセスおよび命令アクセスとユーザ領域へのデータアクセスおよび命令アクセスとを許可する。動作モードがユーザモードのとき検出回路２２１～２２４は、特権領域へのデータアクセスおよび命令アクセスとＡＰＩ領域へのデータアクセスとを禁止し、ＡＰＩ領域への命令アクセスとユーザ領域へのデータアクセスおよび命令アクセスとを許可する。

【００３７】

図１１は動作モード間の遷移を示す図である。

【００３８】

特権モードからユーザモードに遷移する場合、まずＡＰＩ領域に分岐して、特権フラグ２３１をＯＦＦにすることによってＡＰＩモードに遷移する。このとき、特権領域上で特権フラグ２３１をＯＦＦにするとＡＰＩモードに遷移するが、特権領域への不正アクセスとなり割り込みが発生する。ＡＰＩモードへの遷移後、ユーザ領域に分岐することによって、ユーザモードに遷移する。

【００３９】

ユーザモードから特権モードに遷移する場合、まずＡＰＩ領域に分岐した後に、特権フラグ２３１をＯＮにすることによって、特権モードに遷移する。

【００４０】

図１２はメモリアクセス時のフローチャートである。

【００４１】

ユーザモードのとき、メモリアクセスが特権領域へのアクセスの場合（ＳＴ４１でＹＥＳ）、不正アクセスとして割り込みが発生する（ＳＴ４２）。ＡＰＩ領域へのアクセスの場合（ＳＴ４３でＹＥＳ）、データアクセスであれば（ＳＴ４４でＹＥＳ）、不正アクセスとして割り込みが発生し（ＳＴ４５）、命令アクセスであれば（ＳＴ４４でＮＯ）ＡＰＩ

領域への命令アクセスを実行する（ＳＴ４７）。ユーザ領域へのアクセスであれば（ＳＴ４６）、アクセスを実行する（ＳＴ４７）。

【００４２】

ＡＰＩモードのとき、メモリアクセスが特権領域へのアクセスの場合（ＳＴ５１でＹＥＳ）、不正アクセスとして割り込みが発生し（ＳＴ５2）、それ以外の領域へのアクセスであれば（ＳＴ５３）、アクセスを実行する（ＳＴ５４）。

【００４３】

特権モードのとき、どの領域に対しても制限なくアクセスを実行する（ＳＴ５５）。

【００４４】

図１３はモード遷移時のパイプラインチャート図である。ユーザ領域からＡＰＩ領域への分岐の際に、ユーザモードでのＡＰＩ領域へのメモリアクセスが発生するが命令アクセスであるのでアクセスは許可される。また、ＡＰＩモードでの特権フラグのセットによって特権モードに遷移する。

【００４５】

＜効果＞

第２の実施形態によれば第１の実施形態におけるのと同様の効果が得られる。さらに、ユーザ領域から特権領域への分岐の際には「ＡＰＩ領域での特権フラグへのデータアクセス」が必要となるため、特権モードに遷移する前に必ずユーザ領域でのメモリアクセスが完了することになる。

【００４６】

（第３の実施形態）

＜ＩＣカードの全体構成＞

第３の実施形態によるＩＣカードの構成を図１４に示す。このＩＣカードは、図７に示したＩＣカードの構成に加えてさらに検出回路２２５と、ユーザフラグ２４０と、ユーザフラグ判定回路２５１とを備える。

【００４７】

ユーザフラグ２４０はＮ個のフラグ（ユーザフラグ１～ユーザフラグＮ）を含む。

【００４８】

ユーザフラグ判定回路２５１は、ユーザフラグ２４０の出力に従ってユーザフラグ１～ユーザフラグＮのＯＮ／ＯＦＦを判定し、判定結果（ユーザフラグ１～ユーザフラグＮがＯＮであるかＯＦＦであるか）を示す信号Ｓ９を出力する。

【００４９】

モード決定回路２１５は、実行領域判定回路２１４からの信号Ｓ２と特権フラグ判定回路２３２からの信号Ｓ８とユーザフラグ判定回路２５１からの信号Ｓ９とに基づいて動作モードを決定する。

【００５０】

検出回路２２５は、ＣＰＵ２０１からユーザフラグ２４０（ユーザフラグ１～Ｎ）へのアクセスアドレスと信号Ｓ３～Ｓ４とに基づいて、ＣＰＵ２０１からユーザフラグ２４０（ユーザフラグ１～Ｎ）へのアクセスを許可／禁止する。アクセスを禁止するとき検出回路２２５は検出信号Ｓ６を出力する。

【００５１】

＜論理アドレス空間＞

図１４に示したＩＣカードの論理アドレス空間を図１５に示す。ここではＲＡＭ２１２およびフラッシュメモリ２１３のユーザ領域がＮ個の領域（ユーザ領域１～ユーザ領域Ｎ）に分割される。さらにアドレスａ１６～ａ１６＋Ｎがユーザ領域１～Ｎに割り当てられる。ユーザフラグ１～Ｎにアドレスａ１６（ユーザ領域１）～ａ１６＋Ｎ（ユーザ領域Ｎ）が割り当てられる。

【００５２】

＜メモリ保護機能＞

次に、図１４に示したＩＣカードの動作について説明する。ここでは第１および第２の実

施形態と異なる部分について説明する。

【００５３】

モード決定回路２１５は、動作モードを示す信号Ｓ３を出力する。図１６に示すように、実行領域判定回路２１４からの信号Ｓ２が特権領域またはＡＰＩ領域を示しかつ特権フラグ判定回路２３２からの信号Ｓ８が特権フラグ２３１がＯＮであることを示すときモード決定回路２１５は、特権モードを示す信号Ｓ３を出力する。なお、ユーザフラグ１～ＮはＯＮであってもＯＦＦであってもかまわない。信号Ｓ２がＡＰＩ領域を示しかつ信号Ｓ８が特権フラグ２３１がＯＦＦであることを示すときモード決定回路２１５は、ＡＰＩモードを示す信号Ｓ３を出力する。なお、ユーザフラグ１～ＮはＯＮであってもＯＦＦであってもかまわない。信号Ｓ２がユーザ領域１を示しかつ信号Ｓ８が特権フラグ２３１がＯＦＦであることを示しかつ信号Ｓ９がユーザフラグ１がＯＮでありユーザフラグ２～ＮがＯＦＦであることを示すときモード決定回路２１５は、ユーザモード１を示す信号Ｓ３を出力する。同様に、信号Ｓ２がユーザ領域Ｍ（２≦Ｍ≦Ｎ）を示しかつ信号Ｓ８が特権フラグ２３１がＯＦＦであることを示しかつ信号Ｓ９がユーザフラグＭがＯＮでありユーザフラグ１～Ｎ（ただしＭを除く）がＯＦＦであることを示すときモード決定回路２１５は、ユーザモードＭを示す信号Ｓ３を出力する。このように、デコードステージで処理されている命令が格納されている領域（実行領域）と特権フラグ２３１のＯＮ／ＯＦＦとユーザフラグ１～ＮのＯＮ／ＯＦＦとに基づいて動作モードが決定される。

【００５４】

検出回路２２１～２２５は、モード決定回路２１５からの信号Ｓ３が示す動作モードと、ＣＰＵ２０１からのアクセスアドレスが属する領域（アクセス領域）と、信号Ｓ４が示すアクセス種別（データアクセス，命令アクセス）とに基づいてメモリ２１１～２１３、特権フラグ２３１およびユーザフラグ１～Ｎへのアクセスを許可／禁止する。具体的には図１７に示すように、動作モードが特権モードのとき検出回路２２１～２２５はアクセス領域（特権領域，ＡＰＩ領域，ユーザ領域，ユーザ領域１～Ｎ）およびアクセス種別にかかわらずメモリ２１１～２１３、特権フラグ２３１およびユーザフラグ１～Ｎへのアクセスを許可する。動作モードがＡＰＩモードのとき検出回路２２１～２２５は、特権領域へのデータアクセスおよび命令アクセスを禁止し、それ以外の領域（ＡＰＩ領域，ユーザ領域，ユーザ領域１～Ｎ）へのデータアクセスおよび命令アクセスを許可する。動作モードがユーザモードＭ（１≦Ｍ≦Ｎ）のとき検出回路２２１～２２５は、ＡＰＩ領域への命令アクセスと、ユーザ領域へのデータアクセスおよび命令アクセスと、ユーザ領域Ｍへのデータアクセスおよび命令アクセスとを許可し、特権領域へのデータアクセスおよび命令アクセスと、ＡＰＩ領域へのデータアクセスと、ユーザ領域１～Ｎ（ただしＭを除く）へのデータアクセスおよび命令アクセスとを禁止する。

【００５５】

図１８はモード遷移を表す図である。特権モードのとき、特権領域もしくはＡＰＩ領域上のプログラムを実行中である。特権モードからＡＰＩモードに遷移する場合、まずＡＰＩ領域に分岐し、特権フラグ２３１をＯＦＦにする。ＡＰＩモードからユーザモードＮに遷移する場合、ＡＰＩ領域において、ユーザフラグＮをＯＮにした後にユーザ領域Ｎに分岐する。ユーザフラグＮがＯＦＦの状態でユーザ領域Ｎに分岐した場合、不正アクセスと判定されて割り込みが発生する。次に、あるユーザ領域から別のユーザ領域に遷移する場合を説明する。ユーザ領域Ｎからユーザ領域Ｍ（０＜Ｍ＜Ｎ）に遷移する場合、ユーザフラグＭをＯＮにするためにＡＰＩ領域に分岐（ＡＰＩモードに遷移）する。その後で、ユーザフラグＮをＯＦＦ、ユーザフラグＭをＯＮにし、ユーザ領域Ｍに分岐する。

【００５６】

＜効果＞

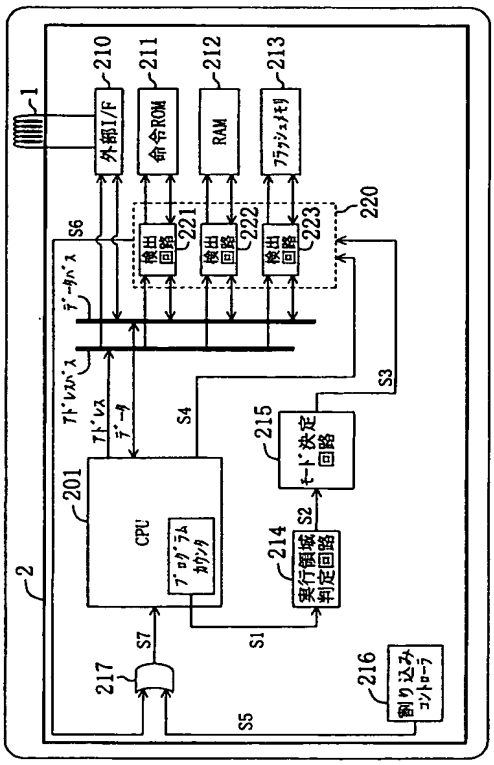
以上のように第３の実施形態によれば、ユーザプログラムから特権領域やほかのユーザ領域への不正なアクセスを防止することができる。

【図面の簡単な説明】

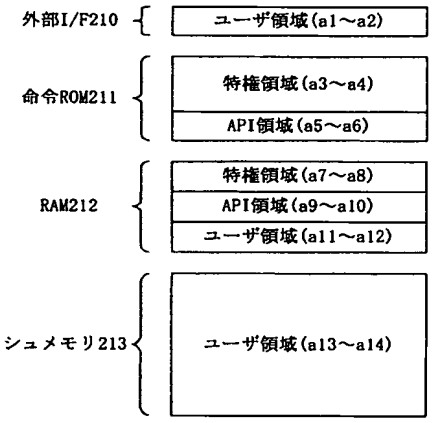
【図１】第１の実施形態によるＩＣカードの全体構成を示すブロック図である。

【図２】図１に示したＩＣカードの論理アドレス空間を示す図である。
【図３】実行領域と動作モードとの対応関係を示す図である。
【図４】各動作モードにおいてアクセスを許可／禁止する領域を示す図である。
【図５】メモリアクセス時のフローチャートである。
【図６】モード遷移時のパイプラインチャート図である。
【図７】第２の実施形態によるＩＣカードの全体構成を示すブロック図である。
【図８】図７に示したＩＣカードの論理アドレス空間を示す図である。
【図９】実行領域および特権フラグと動作モードとの対応関係を示す図である。
【図１０】各動作モードにおいてアクセスを許可／禁止する領域を示す図である。
【図１１】動作モード間の遷移を示す図である。
【図１２】メモリアクセス時のフローチャートである。
【図１３】モード遷移時のパイプラインチャート図である。
【図１４】第３の実施形態によるＩＣカードの全体構成を示すブロック図である。
【図１５】図１４に示したＩＣカードの論理アドレス空間を示す図である。
【図１６】実行領域、特権フラグおよびユーザフラグと動作モードとの対応関係を示す図である。
【図１７】各動作モードにおいてアクセスを許可／禁止する領域を示す図である。
【図１８】動作モード間の遷移を示す図である。
【符号の説明】
２０１　ＣＰＵ、２１０　外部Ｉ／Ｆ、２１１　命令ＲＯＭ、２１２ＲＡＭ（データメモリ）、２１３　フラッシュメモリ（拡張メモリ）、２１４　実行領域判定回路、２１５　モード決定回路、２２０　不正アクセス検出回路群。

【図１】



【図２】



【図３】

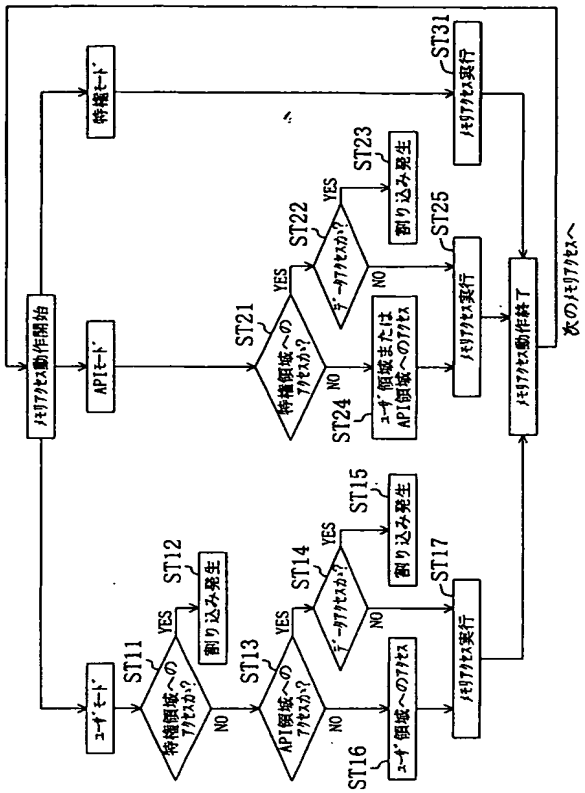
実行領域(S2)	動作モード(S3)
特権領域	特権モード
API領域	APIモード
ユーザ領域	ユーザモード

【図４】

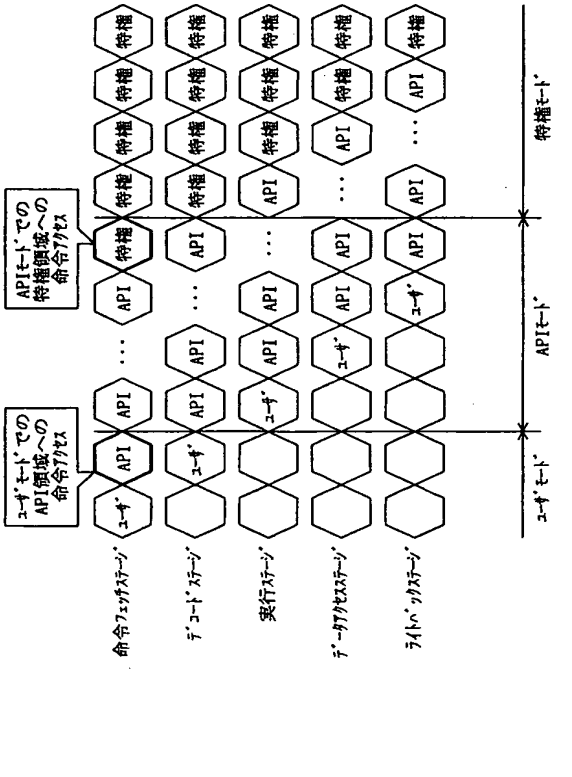
アクセス領域および アクセス種別 / 動作モード	特権領域		API領域			ユーザ領域		
	データ アクセス	命令 アクセス	データ アクセス	命令 アクセス		データ アクセス	命令 アクセス	
特権モード	○	○	○	○		○	○	
APIモード	×	○	○	○		○	○	
ユーザモード	×	×	×	○		○	○	

○・・・許可，×・・・禁止

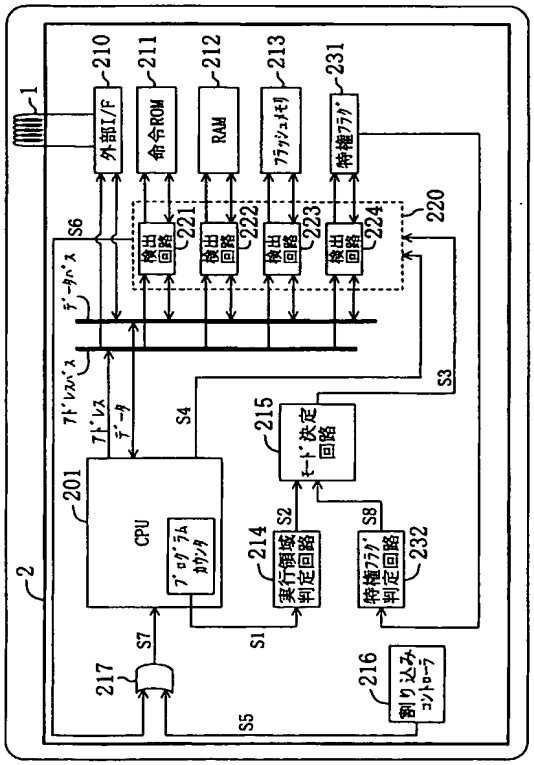
【図５】



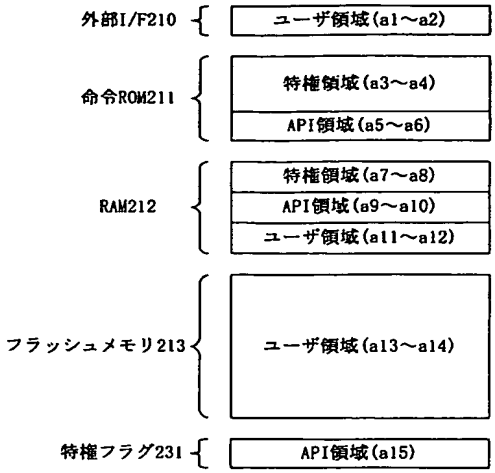
【図６】



【図７】



【図８】



【図９】

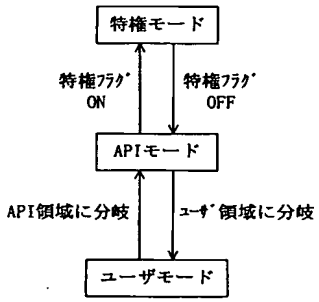
実行領域(S2)	特権フラグ(S8)	動作モード(S3)
特権領域	ON	特権モード
API領域	ON	特権モード
	OFF	APIモード
ユーザ領域	OFF	ユーザモード

【図１０】

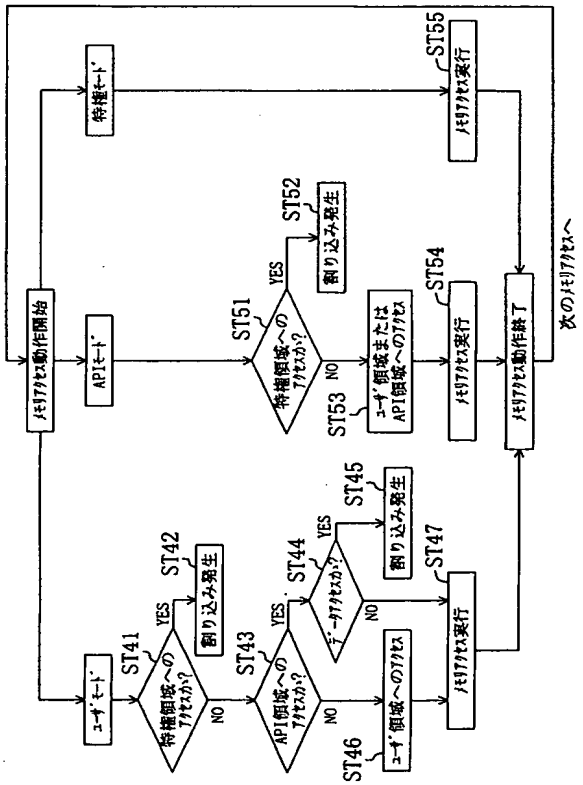
アクセス領域およびアクセス種別 / 動作モード	特権領域 データアクセス	特権領域 命令アクセス	API領域 データアクセス	API領域 命令アクセス	ユーザ領域 データアクセス	ユーザ領域 命令アクセス
特権モード	○	○	○	○	○	○
APIモード	×	×	○	○	○	○
ユーザモード	×	×	×	○	○	○

○・・・許可, ×・・・禁止

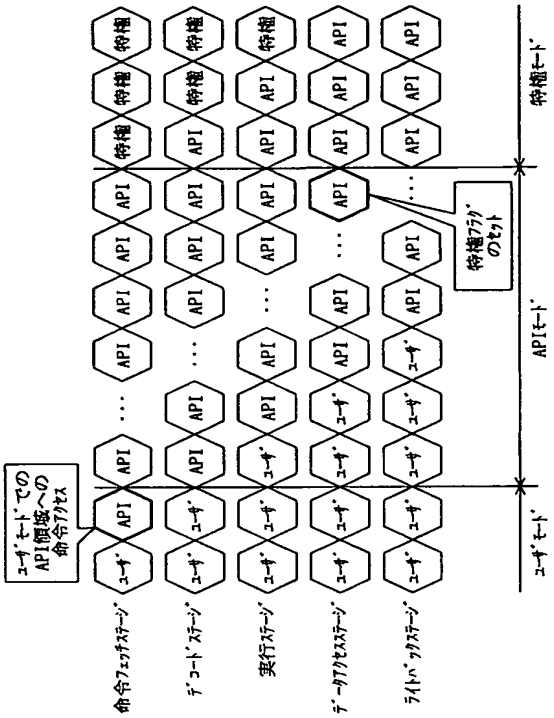
【図１１】



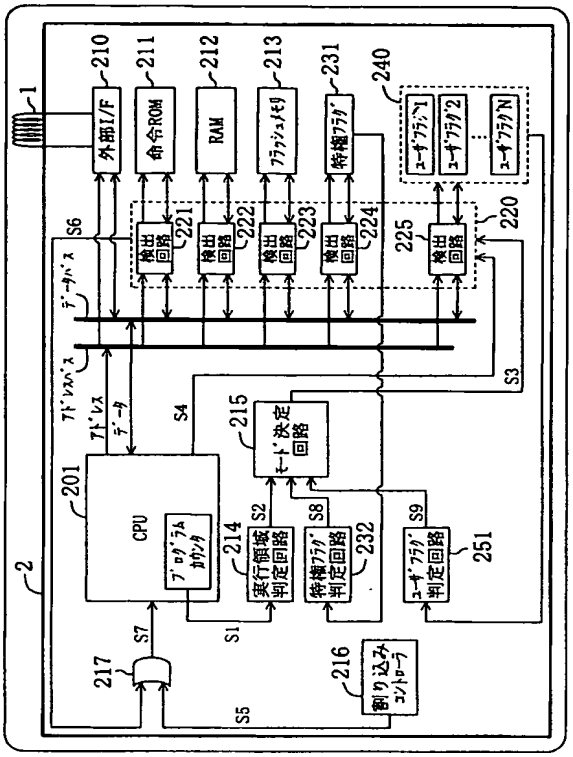
【図１２】



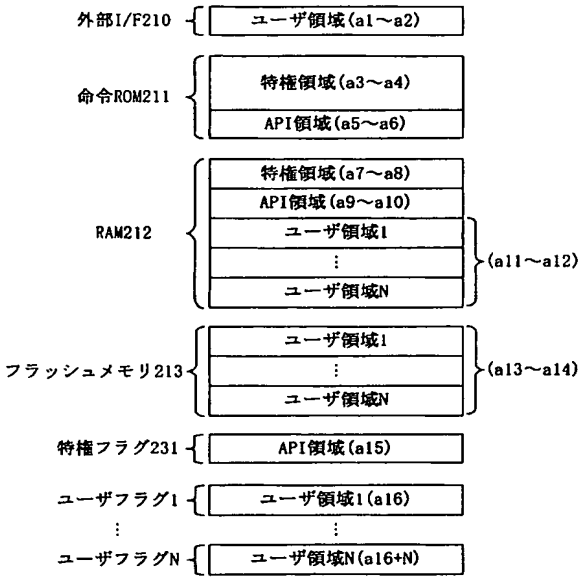
【図１３】



【図１４】



【図１５】



【図１６】

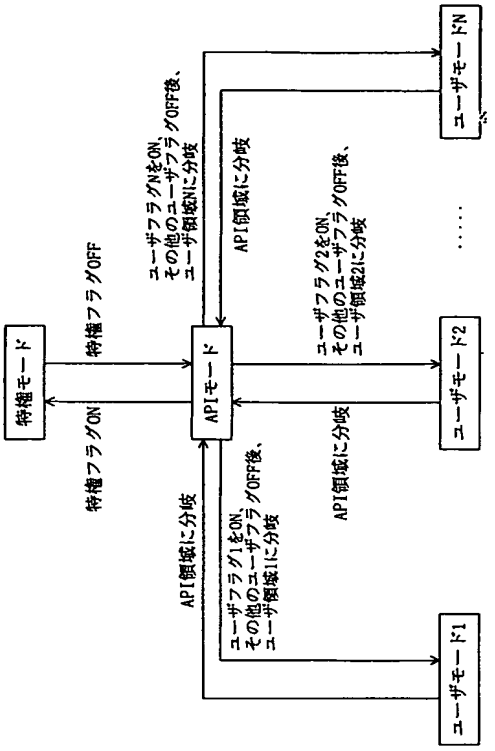
実行領域(S2)	特権フラグ(S8)	ユーザフラグ1	ユーザフラグ2	…	ユーザフラグN	動作モード(S3)
特権領域/API領域						
API領域	ON	ON/OFF	ON/OFF	…	ON/OFF	特権モード
	OFF	ON/OFF	ON/OFF	…	ON/OFF	APIモード
ユーザ領域1	OFF	ON	OFF	…	OFF	ユーザモード1
ユーザ領域2	OFF	OFF	ON	…	OFF	ユーザモード2
…	…	…	…	…	…	…
ユーザ領域N	OFF	OFF	OFF	…	ON	ユーザモードN

【図１７】

動作モード ＼ アクセス領域およびアクセス種別	特権領域		API領域		ユーザ領域		ユーザ領域1		ユーザ領域2		…	ユーザ領域N	
	データアクセス	命令アクセス	データアクセス	命令アクセス	データアクセス	命令アクセス	データアクセス	命令アクセス	データアクセス	命令アクセス	…	データアクセス	命令アクセス
特権モード	○	○	○	○	○	○	○	○	○	○	…	○	○
APIモード	×	×	○	○	○	○	○	○	○	○	…	○	○
ユーザモード1	×	×	×	○	○	○	○	○	×	×	…	×	×
ユーザモード2	×	×	×	○	○	○	×	×	○	○	…	×	×
…	…	…	…	…	…	…	…	…	…	…		…	…
ユーザモードN	×	×	×	○	○	○	×	×	×	×	…	○	○

○・・・許可, ×・・・禁止

【図１８】



フロントページの続き

(74)代理人 100115510
弁理士 手島 勝
(74)代理人 100115691
弁理士 藤田 篤史
(72)発明者 長谷部 朋哉
大阪府門真市大字門真１００６番地 松下電器産業株式会社内

Ｆターム(参考) 5B017 AA01 BA01 BA06 CA11 CA14
5B035 BB09 CA11 CA23 CA38
5B076 FB02